IMPULSE

"Moving S&MA Forward through Information Management"

Published periodically by the Information Management group to inform MSFC S&MA support contract employees of Automated Data Processing issues, procurements, requests and news.

Issue 7 ***** SPECIAL VIRUS EDITION ***** January 1997

COMPUTER VIRUS INFECTIONS SWEEP THROUGH CONTRACT

As Fast As Speeding Email, "Concept", "Impostor" And "Wazzu" Attack
What Is Happening And Where To Turn For Help

What Is Happening?

Recently, a variety of computer viruses have plagued S&MA contract WPS and DDS users. Most of these viruses have been of a type known as "Word Macro Viruses". "Word" refers to Microsoft's word processing application, available in both WPS and DDS. A "macro" is a series of Word commands grouped together as a single command to make everyday tasks easier. A macro typically combines multiple commands to automate a complex series of tasks and / or a frequently used series of repetitive tasks. "Word Macro Viruses" are macros that have been designed with malicious intent.

How Do I Become Infected?

Word records a macro as a series of instructions in its macro language, WordBasic. By default, Word stores macros in the Normal template (NORMAL.DOT) so that they're available for use with every Word document. A local infection begins when the user receives and opens an infected Word document. The infected Word document may arrive as an Email attachment, on floppy or exist on a shared network directory. The malicious macros have been written to execute whenever the infected document is opened by Word. They begin by copying themselves to the Normal template. From that moment on, the Word application itself is considered to be infected.

When you start Word or click the New Document icon, Word creates a new blank document that is based on the Normal template. If the Normal template has previously been infected, that new blank document is infected from its inception. Additionally, any uninfected document (based on the Normal template) that is saved again after the Normal template is infected, will become infected.

How Is The Infection Spread?

An infection spreads when an infected Word document is distributed via Email, floppy or shared network directory.

Inside IMpulse

S&MA INFORMATION MANAGEMENT TROUBLE TICKET / REQUEST FORM SUMMARY

— TO DATE —

529	Total Requests Submitted
522	Requests Closed

What Are The Symptoms Of A Word Macro Virus Infection?

In the absence of virus detecting software to provide an on-screen warning, an infection of a Word macro virus might be detected if Word exhibits strange behavior, for example:

- When executing a "Save As…" action, Word may insist on saving the document as a Word template (with .DOT extension) and not allow the user to change the disk drive and directory in which to save.
- The word "wazzu" may appear randomly in an infected Word document.
- A dialog box may appear with the cryptic message "DMV".

Besides witnessing strange behavior, you may find a macro named "DMV" in the Normal template. To check, select "Tools" from the Word menu bar, then "Macros…" and see if a macro named "DMV" is listed.

Finally, Real-Time Virus Protection

With VSWatch (DDS) or ViruSafe Resident Monitor (WPS) loaded, ViruSafe will warn of infected Word documents when you attempt to open them. (For information on VSWatch and ViruSafe Resident Monitor, see DDS and WPS-specific instructions elsewhere in this issue.) ViruSafe will not allow infected Word documents to be opened as opening would spread the infection to the Word application itself (NORMAL.DOT). Instead, an information box will appear on-screen with details of the infection including the virus' name.

What To Do If You Receive An Infected Email Attachment

In the case of an infected Word document received as an Email attachment:

1. Notify the sender that the attachment is infected.
2. Request that a clean version of the attachment be re-sent to you after the sender's PC has been disinfected.
3. Delete the Email message with the infected attachment.

Where To Turn For Help

- S&MA contractors who are notified they have a virus can submit a trouble to the IM group for assistance; problem: "need help removing virus infection".

- S&MA civil servants who are notified they have a virus can either request assistance from Kelly Carter / RSSC (5-1200) or call the center-wide help desk at 4-1771.

- Civil servants other than S&MAshould call the center-wide help desk at 4-1771.

"Wazzu? Wazzu who? An Impostor?! What a Concept!"

DDS Users (Windows95):

DDS-Specific Anti-Virus Instructions

How To Determine If Your PC Has Memory-Resident Anti-Virus Monitor (Real-Time Virus Protection) Installed

A green, blinking icon will appear next to the clock located on the Windows95 task bar if the memory-resident anti-virus monitoring program is installed and operating.

If the green, blinking icon is not present, the anti-virus monitor is not resident in memory. Submit a trouble ticket to the IM group for assistance; problem: "green, blinking anti-virus monitor icon not present (DDS)".

How To Determine If The Memory-Resident Anti-Virus Monitor Is The Latest Version Available

1. Double-click the green, blinking icon that appears next to the clock located on the Windows95 task bar. The "ViruSafe Watch" dialog box will appear.
2. Click on the "General Information" tab.
3. Locate the "Versions" section of the dialog box.
4. The "VSWatch version:" should be 2.1.

If the VSWatch version is less than 2.1, submit a trouble ticket to the IM group for assistance; problem: "old version of VSWatch (DDS)".

Insure The Memory-Resident Anti-Virus Monitor Is Providing Full Protection

1. Double-click the green, blinking icon that appears next to the clock located on the Windows95 task bar. The "ViruSafe Watch" dialog box will appear.
2. Click on the "Online Protection" tab.
3. Click the "Configure Online" button (found near the bottom right corner of the dialog box). The "ViruSafe 95 Protect Configuration" dialog box will appear.
4. Click the "General" tab.
5. Locate the "Scan Type" section of the dialog box.
6. Select "Full Scan".

WPS Users (Standard Windows):

WPS-Specific Anti-Virus Instructions

How To Determine If Your PC Has Memory-Resident Anti-Virus Monitor (Real-Time Virus Protection) Installed

1. At the MS-DOS prompt, type: C:\VS\VS/T
   The "ViruSafe Resident Monitor 7.2" dialog box should appear. (If, instead, the words "File Not Found" appear, submit a trouble ticket to the IM group for assistance; problem: "ViruSafe software missing (WPS)".)
2. Locate the "VS Monitor Status" at the bottom of the dialog box.
3. The "VS Monitor Status" should be "ON"

If the VS Monitor Status is "Not Installed", submit a trouble ticket to the IM group for assistance; problem: "VS Monitor Status = Not Installed (WPS).".

How To Determine If The Memory-Resident Anti-Virus Monitor Is The Latest Version Available

1. At the MS-DOS prompt, type: C:\VS\VS/T
   The "ViruSafe Resident Monitor 7.2" dialog box should appear. (If, instead, the words "File Not Found" appear, submit a trouble ticket to the IM group for assistance; problem: "ViruSafe software missing (WPS)".)

If the ViruSafe Resident Monitor version is less than 7.2, submit a trouble ticket to the IM group for assistance; problem: "old version of ViruSafe Resident Monitor (WPS)".

Insure The Memory-Resident Anti-Virus Monitor Is Providing Full Protection

"ViruSafe Resident Monitor 7.2" for Windows does not have the "less than full protection" option that "ViruSafe Watch" for Windows95 has. If "ViruSafe Resident Monitor 7.2" is installed, **it** offering "full protection".

Comings and Goings

Hello to **Dave Hieber** (pronounced He - burr). Dave joins the IM group from SCI Systems, where he was a Novell Network Administrator for the Govt. Division's Manufacturing facility. He has experience with Novell 4.x , end user support, PC hardware troubleshooting & repair, database development and a number of operating systems including UNIX and most versions of Windows.

Goodbye to **Michele McCullough** who has left the S&MA contract to pursue other interests in Florida. We wish her well.